ABSTRACT OF THE DISCLOSURE

A communication system including a transmitter, a receiver, and a serial link (for example, a TMDS-like link) in which video data (or other data) are encrypted, the encrypted data are transmitted from the transmitter to the receiver, and the transmitted data are decrypted in the receiver, a transmitter and a receiver for use in such systems, a cipher engine for use in such a transmitter or receiver, a method for operating such a transmitter or receiver to encrypt or decrypt data, and a method for authenticating a receiver prior to transmission of encrypted data to the receiver over a serial link. Each transmitter, receiver, and cipher engine is configured to implement a content protection protocol in a manner that implements at least one and preferably more than one of a class of attack prevention features disclosed herein. In preferred embodiments the invention is employed to encrypt data in accordance with the High-bandwidth Digital Content Protection ("HDCP") protocol, or a modified version of the HDCP protocol.